

## 汽车车身计算机中的安全性能

**作者: Robert Kalman**

飞思卡尔半导体公司微处理器应用工程师

### 背景

开车是一件非常危险的事情。对于跳伞运动员来说，最危险的实际上是开车从家到机场这段路程。2002年，欧洲总共有46000多人死于车祸。这个数字比这一地区的艾滋病、脑膜炎、吸毒、哮喘和暴力犯罪及火灾的死亡总人数还要高<sup>1</sup>。

政府对这一统计数字感到非常震惊，多年来一直试图通过诉讼方式，改进这些车辆的安全状况，预防其对公众造成的伤害。自英国于1861年第一次制定出每小时不超过10英里<sup>2</sup>的速度限制，到美国最近制定胎压监测立法（这部法律将于2007年8月生效实施<sup>3</sup>），人类就从未停止旨在提高道路安全的努力。

不仅仅是政府感到有义务改进车辆的安全性能，公众也非常想购买更为安全的汽车。因此，汽车行业一直在朝这个方向努力。NCAP最近的调查<sup>4</sup>显示，安全性能是继价格和功能之后，消费者在购买新车时最关心的问题。

在NCAP测试中达到4星或4星以上的安全性能评级，可以将严重或致命伤害的几率减少30%<sup>5</sup>。这清晰地表明，消费者对更为安全的汽车功能的需求日益增加，并且这些安全功能在挽救生命方面也变得越来越有效。

---

1 World Health Organisation Report for 2003. <http://www.who.int/whr/2003/en/index.html>

2 History of Motoring and Licensing in the UK. [http://www.dvla.gov.uk/histm\\_1/earlyday.htm](http://www.dvla.gov.uk/histm_1/earlyday.htm)

3 National Highway Traffic Safety Administration 49 CFR Parts 571 and 585

<http://www.nhtsa.dot.gov/cars/rules/rulings/TPMSfinalrule.6/TPMSfinalrule.6.html>

4 NCAP commissioned MORI consumer survey

[http://www.euroncap.com/content/media/press\\_releases/november\\_29\\_2005\\_survey1.html](http://www.euroncap.com/content/media/press_releases/november_29_2005_survey1.html)

5 NCAP study based in Sweden on the correlation between NCAP results and actual fatalities

[http://www.euroncap.com/downloads/test\\_procedures/area\\_4/swedish\\_study.doc](http://www.euroncap.com/downloads/test_procedures/area_4/swedish_study.doc)

第一辆在 NCAP 安全标准中获得 5 星的汽车是 2001 年 3 月生产的雷诺 Laguna<sup>6</sup>，其它汽车的安全标准也接近 5 星，这表明不但乘客和司机的安全保护得到较大提高，行人的安全也有了保障。

### 所面临的问题

随着当今生产的汽车越来越多地加入电子元器件，很显然，这些系统的安全也变得越来越重要。飞机早在几年前就开始使用“线控飞行”系统，但它目前还没有遇到汽车行业所面临的价格压力。一些航空系统经常使用系统的冗余性，对一些特定系统，有时甚至达到了“四倍冗余”<sup>7</sup>。汽车行业向自己发出挑战，它必须在不增加汽车成本的情况下达到类似的水平。现在，该是一级制造商及其供应商提出创新解决方案，以极具竞争力的价格解决重要的安全问题的时候了。

### SIL 水平

1998 年，IEC 发布了 61508 标准。该标准中包含一些如何把电子系统中的故障降到最低限度的要求。它给出了系统完整性或其“SIL”水平的几个定义。根据每小时出现的危险故障的几率，可以对应用和系统进行如下分类：

安全完整性水平	每小时发生危险故障的几率
SIL4	$\geq 10^{-5}$ to $< 10^{-4}$
SIL3	$\geq 10^{-4}$ to $< 10^{-3}$
SIL2	$\geq 10^{-3}$ to $< 10^{-2}$
SIL1	$\geq 10^{-2}$ to $< 10^{-1}$

<sup>6</sup> Phase 8 of NCAP testing results

[http://www.euroncap.com/content/media/press\\_releases/phase\\_8.html](http://www.euroncap.com/content/media/press_releases/phase_8.html)

<sup>7</sup> Meeting the challenges of drive by wire electronics. <http://mira.atalink.co.uk/articles/104>

1 FIT (Failure In Time)就相当于每小时的危险故障几率为  $10^{-9}$ ，因此，完整的系统必须在设备的安全预算内，其中，FIT 的总累积数就是 SIL 水平的描述。

决定应用要求的 SIL 水平绝不是一件简单的工作。很显然，飞机的关键系统至少需要符合 SIL3，在有些情况下甚至要求 SIL4。在汽车中，它表现得没这么明显。但有很多这样的例子，如线控转向或线控制动等，它们明显都要求这样的高水平。系统还提供几种工具，用于分析系统所需的 SIL 水平。本文无意为不同的系统分配不同的 SIL 要求，只是说明当今的汽车中有几个必须认真考虑的关键的安全系统。

很明显，汽车的操纵和制动系统最为重要。但是，汽车的照明系统或风挡刮水器的重要程度如何呢？在雨天，什么样的 FIT 水平是系统控制风挡刮水器所能接受的呢？哪些系统“与安全有关”已越来越不成问题，越来越多的问题是，还有没有不安全的系统。

当今汽车中的大多数系统都连接在 CAN 总线或 LIN 子总线上。这就带来了进一步的问题：在一些非关键应用（如 GPS）上的任何错误如何能够传播到另外一个系统（如车门模块）或另一个关键应用上。是不是车内的每个系统都应该最少有 SIL2 级？

可以肯定的是，随着车身计算机融入了越来越多的功能，对这些应用的 SIL 评级的关注也将变得更为强烈。市场上有 OEM 将方向盘锁融入网关或 BCU 的事例。很显然，如果方向盘由于系统故障而被锁住，那么造成的结果就可能是灾难性的，这就导致某些 BCU 系统要求 SIL3 的状态。

### **软件是谁写的？**

在目前的环境中，应用开发人员面临的另一个问题就是软件开发问题。自从软件不再是由一个团队而是由来自几家不同公司的几个团队编写的以来，这个问

题就一直存在。CAN 驱动软件可能来自一家厂商，新运算法则可能来自于另外一家专业公司，而特定标准应用的算法可能又由 OEM 和/或一级供应商编写。有了这些来自不同来源的混合软件，OEM 日益密切关注这些问题就不足为奇了。

事实证明，软件缺陷也越来越成为一个重要问题。2000年，Marcus和Stern就已经指出，40%的系统故障都是由软件缺陷引起的<sup>8</sup>。随着软件复杂性的增加以及软件供应商数量的增长，软件缺陷将来肯定会成为更为重要的问题。

### 飞思卡尔的先进产品

新的飞思卡尔 S12X 产品系列提供了众多新一代汽车车身计算机所要求的功能。在为现有解决方案提供一条降低成本的路径的同时，还为未来的 BCU 提供了众多优势。

S12X 系列具有减轻故障向系统中的其它设备扩散的功能。其时钟监控和电压监控功能得到了极大的改进，因此可以快速有效地响应系统中的故障。这些功能允许微控制器监测振荡器的问题，并代以从内部时钟运行。这不但消除了对另一个时钟的需要，还使微控制器能连续监控振荡器，把振荡器从“安全”状态恢复到“正常”状态。

对来自多家厂商的软件包的担心还可以通过系统对 MPU 的应用而得到缓解。MPU 可以预防软件应用程序中的系统错误，有助于确保它们只能看、读和写到手头中任务的特定存储位置。

S12XE 中令人印象最深的改进可能就是 Xgate 了。这颗很小的协处理器运行在完全不同于 S12X 核心的指令集上。它的运行独立于 CPU，此外，它还非常灵活，配置后可以开展多种不同的活动，如额外的内部看门狗，从而有利地补充

---

<sup>8</sup> E. Marcus and H. Stern. Blueprints for high availability: Designing Resilient Distributed Systems.

了已经投入使用的计算机正常运行 (COP) 模块。它还可以在配置后运行与 CPU 一样的算法（或不同的版本），从而确保算法的正确执行，在无需任何其它组件的情况下提供设备的冗余性检查。

Xgate 是一个全能型解决方案，它也可以进行配置，以运行“非关键的”应用程序，允许 CPU 只处理一些“关键”任务，因此提高了对系统中的其它部分的错误的响应速度。

S12XE 系列的详细资料有望于 2006 年中期在产品正式推向市场后，从您当地的飞思卡尔经销商那里获得。

## 结论

标准的出现是为了满足日益复杂的电子系统的要求。新的 IEC61508 标准非常有助于为这些要求提供更为严格的背景。随着汽车 OEM 努力在降低成本的同时改进质量和安全性，就不再是只将制动和操纵系统之类的系统置于这些标准的监管之下了。

安全问题正越来越多地成为人们讨论的热点，即使是在汽车的车身领域也不例外。飞思卡尔一直致力于提供高性能、经济高效、非常适合于车身计算机市场的器件。毫无疑问，于 2006 年中期推向市场的 S12XE 系列新产品，将促使飞思卡尔在这一竞争市场居于前沿地位。